Information Technology Security Standards

Adopted by the Information Services Board (ISB) on November 20, 2000

Policy No: 401-S1
Supersedes No: N/A
Effective Date: November 20, 2000
Revision Date: March 2003

Also see: 400-P1, 402-G1
Auditor's Audit Standards
OFM Guidelines for Economic Feasibility
Definitions

Table of Contents

Introduction

To implement the Information Technology (IT) Security Policy, adopted by the Information Services Board (ISB) on July 14, 2000 to protect IT resources, and enable security audits of those resources, it is required that agencies adhere to common IT security standards. Common standards will help ensure that all agencies have an

effective and secure environment for IT processing. The standards contained herein are built upon those previously addressed in the IT Security Policy dated November 1997 and the current policy. Additional standards have been added to protect against the Internet-related threats described below.

Research and industry sources have identified and categorized threats to information security based upon documented breaches at a variety of organizations in the public and private sectors. Sources of threats include:

- Employees or contracted vendors who allow accidental disclosure of information, or who abuse their privileges and access information for spite or profit
- Unauthorized intruders who mount attacks to gain unauthorized access to information, damage files or systems, or disrupt operations
- Persons who use credit cards fraudulently
- Presentation of commercial certificates of authentication granted by dishonest or ineffective certificate authorities

According to commonly accepted National Institute of Standards and Technology (NIST) documentation (see ***Engineering Principles for IT Security (EP-ITS)*** (http://csrc.ncsl.nist.gov/), types of threats in an Internet environment include:

- Component Failure - Failure due to design flaws or hardware/software faults that can lead to denial of service or security compromises through the malfunction of a system component. Downtime of a firewall or false rejections by authorization servers are examples of failures that affect security
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users may occur through a variety of mechanisms: misrouted electronic mail, printer output, mis-configured access control lists, group IDs, etc.
- Misuse - The use of information assets for other than authorized purposes can result in denial of service, increased cost, or damage to reputations. Internal or external users can initiate misuse
- Unauthorized deletion, modification or disclosure of information - Intentional damage to information assets that results in the loss of integrity or confidentiality of business functions and information
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization

The protection of computer systems and related data in the State of Washington requires an approach that results in implementation of a balanced, cost-effective application of security disciplines and techniques required by these standards.

Security standards define the processes, procedures, and practices necessary for implementing an agency-specific IT security program. Standards apply to all IT activities related to computers and voice, data, or video communications, whether they are operated by or for an agency. They include specific steps that must be taken to ensure that a secure Internet environment is maintained and electronic commerce (E-commerce) initiatives provide for privacy and security of confidential information.

At the core of these standards is the concept of a shared, trusted environment for interaction between agencies as well as agency to customer transactions. This shared, trusted environment is defined as the Washington State Digital Government framework. This environment will be created and maintained by the use of agreed to common security mechanisms, policies, and training in the key areas of:

- Authentication and access control
- Encryption
- Internetworking and Virtual Private Networks

Agencies that operate some or all of their information systems outside of this environment must still adhere to the security principles contained in these standards by creating equivalent environments.

This document contains the following IT security standards:

- Standards for Agency IT Security Program Development and Maintenance
- Standard for WWW Browser/Web Server Configuration
- Standards for Digital Government (Internet) Application Packet Submittal
- Standards for Secure Exchange of Information
- Standards for Wireless LAN Access

Table 1 provides a cross-reference of the IT Security Policy to the relevant section on the IT Security Standards.

Table 1

Cross-reference of IT Security Policy and Standards

Policy	Relevant Standard Section
1. Each agency must operate in a manner consistent with the maintenance of a shared, trusted environment.	E.4 Network and Telecommunication Security E.5.b Internet Access Security
2. Each agency must establish its networks and secure applications within the Washington State Digital Government framework. This requires that all parties interact with agencies through a common security architecture and authentication process	E.4 Network and Telecommunication Security E.5.b Internet Access Security
3. Each agency that operates its applications and networks within the Washington State Digital Government framework must subscribe to the principles of shared security	E.4 Network and Telecommunication Security E.5.b Internet Access Security
4. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses	All E-Commerce specific standards
5. Each agency must ensure staff is appropriately trained in IT security procedures	F. IT Security Program Training Standards
6. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment	G. IT Security Program Maintenance Standards
7. Each agency must conduct an IT Security Policy and Standards Compliance Audit once every three years. It must be performed by parties independent of the agency's IT organization	G. IT Security Program Maintenance Standards IT Security Audit Standards developed and promulgated by the Office of the State Auditor
8. Pursuant to RCW 43.105.017(3), agency heads will confirm in writing that the agency is in compliance with this policy	G. IT Security Program Maintenance Standards
9. The State Auditor may audit agency IT security processes, procedures, and practices	G. IT Security Program Maintenance Standards IT Security Audit Standards developed and promulgated by the Office of the State Auditor

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards, and procedures.

Scope

These standards apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

Exemptions

This policy applies to Institutions of Higher Education, except, pursuant to RCW 43.105.200, when they develop security policies in lieu of the policy statements below that are: a) appropriate to their respective environments, and b) consistent with the intent of the Information Services Board. Such higher education security policies must address:

- Appropriate levels of security and integrity for data exchange and business transactions;
- Effective authentication processes, security architecture(s), and trust fabric(s); and
- Compliance, testing and audit provisions.

Standards

I. Standards for Agency IT Security Program Development and Maintenance

A. Section Overview

This section contains instructions to facilitate the development and maintenance of agency IT security program components needed to protect the integrity, availability, and confidentiality of agency data and safeguard agency IT resources.

Topics covered in this section include:

- Agency IT Security Policies and Standards
- Business impact analysis and risk, threat and vulnerability analyses
- IT Security strategy
- IT Security program components
- IT Security training
- IT Security program maintenance

B. Agency IT Security Policies and Standards

1. Agencies may adapt these standards to meet individual needs, but their security program must address all applicable elements outlined in this section, most importantly it must recognize the importance of an enterprise approach to IT security. The amount of detail included in an agency program should be commensurate with the size, complexity, and potential business exposure of the installation and the agency. An Agency IT security program must contain enough information to:
   a. Enable agency management to assure the agency's ability to protect the integrity, availability, and confidentiality of agency information, and
   b. Protect its IT assets from unauthorized use or modification and from accidental or intentional damage or destruction.

2. An agency's IT security program must appropriately reference other organization's IT security information if the agency shares common software, hardware, telecommunication systems, inter-networked, or Internet-based systems with that organization. In addition, the program must cover procedures that affect the design, availability, or operation of IT resources within the agency. Each agency shall have appropriate inter-organizational agreements in place to support review by Department of Information Services (DIS) and/or the Office of the State Auditor.
3. If an agency purchases IT services from another organization, the agency and the service provider will work together to make certain the IT security standards for the service provider fit with the agency's security program. If two or more agencies participate with each other in operating an information service facility, the agencies must develop joint IT security program components that meet their mutual needs.
4. All IT security program documentation should be written in a clear, compelling, non-technical manner.

CAUTION:
IT security program documentation may contain sensitive information about the agency's business, communications, and computing operations or employees. Such information should be shared only with personnel who have a need to know.

C. Business Impact and Risk, Threat and Vulnerability Analysis

1. A business impact and risk, threat, and vulnerability analysis shall be performed for all significant fiscal and mission critical applications and systems as well as systems containing confidential or sensitive information. The purpose of the business impact analysis and risk, threat, and vulnerability analysis should include focus on security and is to help the agency identify its principal security exposures. These analyses:

a. Summarize the operational, legal, and financial impact that could result from a disruption affecting IT resources of the agency; and

b. Document the threats that could result in the intentional or accidental destruction, modification or release of data, computer or telecommunication resources of the agency.

2. When Internet-based IT service mechanisms are involved, agencies must conduct a specific risk analysis to determine the appropriate authentication, access control, and encryption requirements based on the related Network and Telecommunications Security standards (See Section E.4. page 11). Specific content areas for the required Internet authentication risk analysis can be found in the Internet Access Security section E.5.b. of this document.

3. Instructions and suggested format for completing a Business Impact Analysis and Risk, Threat and Vulnerability Analysis will be found in Section 1 of the Information Technology Security Guidelines.

D. IT Security Strategy

The purpose and focus of developing an IT security strategy is to define the level of protection that should be accorded to agency information assets. This is typically determined by a combination of federal and state laws and regulations and industry best practices. In general, information assets processed and stored by various state agencies range on a continuum from information that is freely available to the general public on the low end to sensitive or legally private information on the high end. Public information must be protected only to the extent that it cannot be surreptitiously changed. Information on the higher end of the continuum, e.g., health related information, the Address Confidentiality Program, and other information specifically made exempt from public disclosure, requires a very high degree of protection. Accordingly, protective measures should be workable, cost effective and commensurate with the level of protection required by law and suggested by prudence.

An agency's security strategy must provide an overview of the process that the organization has adopted to protect its data and IT assets. It should summarize the general security strategy of the agency, at a minimum addressing how the agency has complied with the following:

1. Establishing agency security practices for IT personnel, users of computer services, and anyone else who has access to sensitive or confidential information. Practices must emphasize the importance of preventing unauthorized access, misuse, modification, damage to, or loss of IT hardware, software, data, and facilities. Practices must describe actions to be taken for failure to observe security rules and procedures. For example, describe the disciplinary action to be taken for a password sharing violation.

Agencies must also identify a security awareness process that will be used to ensure that all IT personnel, users of computer services, and others having access to sensitive or confidential information are aware of the security practices used by the agency.

In addition, the strategy must address how the agency will ensure secure interactions will take place within an environment consistent with this standard and, if relevant, how these transactions will utilize a common authentication process, security architecture, and point of entry.

2. Assigning responsibility for IT security to an individual or group with the appropriate training and background to administer the functions. Ensure the individual or group has proper authority to install, monitor, and enforce security rules and procedures.

3. Specifying physical security arrangements and controls that are appropriate for the size and purpose(s) of the installation.

4. If involved in E-commerce, addressing specific strategies relating to the following potential Internet-based security exposure:
   - Component failure
   - Information browsing
   - Misuse
   - Unauthorized deletion, modification or disclosure of information
   - Penetration
   - Misrepresentation

E. IT Security Program Components

Document standards and procedures for the functional areas outlined below and, where relevant, describe prevention, detection and response practices for appropriate areas. The following five areas must be covered by an agency's security program:

- Personnel Security
- Physical Security
- Data Security
- Network and Telecommunications Security
- Access Security

1. Personnel Security

a. Agencies must develop, document, and implement processes for the selection, orientation, and supervision of employees and contractors. The objective is to ensure that a high level of integrity and satisfactory staff conduct is achieved and maintained, and to promote an awareness of security matters. Include the following:

- Hiring practices
- Reference checks
- Security awareness training
- Security program training
- Employee performance requirements
- Vendor and service personnel monitoring
- Background checks where appropriate

b. Suggested guidelines for developing and implementing a personnel security program can be found in Section 2 of the Information Technology Security Guidelines.

2. Physical Security

a. Agency management is responsible for assuring that adequate protective measures are implemented for all IT computing resources. The purpose of the physical security component of the IT security program is to reduce the risk of compromise of data due to physical break-ins or unauthorized access to server resources. Physical security topics that must be addressed by an agency security program include:

- Location and layout of the facility
- Physical security attributes for computer or telecommunications rooms (if applicable)
- Facility access control
- Data storage and telecommunications controls
- Off-site media storage
- Mobile/remote computing security control
  - Laptops
  - Data Storage Devices

b. Suggested guidelines for developing and implementing a physical security program can be found in Section 3 of the Information Technology Security Guidelines.

3. Data Security

a. Develop, document, and implement a security program component that is appropriate for the level of sensitivity/confidentiality of the information being processed. The purpose of the data security component of the IT security program is to reduce the risk associated with the compromise or destruction of agency-controlled data. Content should include rules for the storage and dissemination of data shared with other organizations. The data security program component must address the following:

- Agency data security policy statements
- Software version control and its currency
- Access control techniques
- Data entry processes
- Processing accuracy
- Distribution of output reports and introduction or release of data
- Data and program back-up
- Controls to prevent unauthorized use or removal of tape files, diskettes, and other media
- Data encryption standards for storage and secure management
  - Document risk assessment processes
  - Document conditions, mechanisms, and attributes associated with the agency encryption plans
- Processing audit trails
  - Regular reviews of access audit logs
  - Support to real-time monitoring activities
- Application testing
- System access violations
  - Immediate response (shut downs, tracking, etc.)
  - Notification and communication procedures
  - Trend analysis
- Intrusion detection – notification and response procedures
- Virus prevention, detection, and removal procedures
- Appropriate disposal of hardcopy data which may contain sensitive information or information which may allow compromise of information systems security

b. Instructions and suggested format for the content of the data security program component can be found in Section 4 of the IT Security Guidelines

4. Network and Telecommunications Security

a. Develop, document, and implement a security program component for network and telecommunications controls that address access authorization, equipment approval, change control, and operational and physical security controls.

Specifically, document the agency's security plans as they relate to each of the following categories:

- Network and telecommunications management – specifically document how the agency operates its applications and establishes secure network sessions within the Washington State Digital Government framework
- Internetworking servers, network infrastructure equipment and data transmission within agency intranet and extranet environments, including remote access to applications in these areas
- Physical network infrastructure
- Secure location of communications equipment to prevent theft and tampering
- Terminal, Remote Job Entry (RJE) and network node (bridges, routers, etc.) access security (including Telnet, RLOGIN, GDP, etc.)
- Controls to prevent the introduction of unauthorized programs into computer systems
- Network breach detection and incident response, to include use of intrusion detection tools
- Remote access services, including remote access to e-mail
- Wireless communications, including radio frequency and other transmission systems

b. If an agency uses Virtual Private Networks (VPN) services, the agency's security program must address the methodology used.
    1) VPN solutions must use industry standard protocols
    2) If an agency operates a VPN solution through a firewall configuration other than Fortress, they must use an equivalent solution and document the configuration in the agency security program documentation
    3) If an agency operates a VPN solution that involves token-based technology such as SmartCards, they must use the mechanisms supported by the Washington State Digital Government framework or an equivalent solution. Equivalent solutions must be documented in the agency security program documentation

c. Suggested guidelines for implementing telecommunications operational and physical security program components can be found in Section 5 of the Information Technology Security Guidelines

5. Access Security

a. General Access Security

1) Develop, document, and implement a security program component for access security controls over mainframe, client/server, Internetworked, wireless LANs and stand-alone workstation-based systems consistent with the critical nature of the data processed. Document the access security practices in the agency as they relate to each technology category.

2) Hardened passwords should be used whenever technically and operationally feasible. Appropriate user training should be considered regarding the physical protection of hardened passwords that may be more difficult to remember. For those systems for which it would be technically infeasible or which would require modification to meet this requirement as defined below, agencies must document what other measures are to be taken to secure user access.

   Hardened Passwords must meet the following criteria:

   - Passwords must be a minimum of 8 characters long and contain at least one special character and 2 of the following 3 character classes: upper case letters, lower case letters, and numerals
   - Must not contain your user name or any part of your full name
   - Passwords must be changed a minimum of every 120 days
   - If possible, password administration rules must be systematically enforced

3) Additional requirements include processes for:

   - Controlling use of dial-up lines. Dial-in ports should only be used if there is no other way to satisfy a business need. If dial-in is used, all security features (dial back, etc.) appropriate to the operating environment should be used
   - Establish “lock-out” mechanisms to be activated after a maximum of up to five unsuccessful authentication attempts
   - Protecting voice telecommunication State Controlled Area Network (SCAN) authorization codes for access to long distance dialing
   - Recording telecommunications accesses
   - Monitoring hardware and software vendor access lines to computer and telecommunications systems

b. Internet Access Security

The introduction of the Internet as an access alternative to applications and data may impose new risks regarding the verification of an end user's identity. The standards set forth in this section respond to the issues that must be addressed by agencies concerned with authentication and access of Internet-based systems developed in support of e-government initiatives. **Authentication** is defined as the process of establishing and verifying the identity of a user. **Access control** determines an authenticated party's rights to access applications and data. Once a party is authenticated, access control to specific applications and data is solely within the domain of the agency administering the application or data. Access control is, however, an integral part of an agency's security program and the tools and processes used should be appropriately documented.

Authentication Levels of Confidence

E-commerce and Internet-based applications must involve the use of authentication processes and mechanisms that provide a level of identity confidence (level of confidence) that is commensurate with the risk associated with unintended access and/or disclosure of data. Levels of identity confidence fall on a continuum from very high to very low. If the risk associated with access and/or disclosure by an unauthorized user would result in significant financial damage or release of restricted material, it may require a high level of confidence before access is permitted. When information is public in nature and access is permitted widely, a very low level of confidence, or no identification of a party seeking access, may suffice.

The level of identity confidence (level of confidence) is determined by the degree of diligence attributable to the processes and mechanisms used in authenticating a user. Specifically, "Level of Confidence" can be defined by the cumulative value of the processes, controls, mechanisms and technologies used in the authentication process to provide the following:

1) **Identification and Authentication.** To initially establish and confirm the identity of an individual or entity and ensure that an authentication mechanism (e.g. digital certificate, password, etc.) used to authenticate an individual or entity has been securely issued.
2) **Authentication Integrity**. To ensure that the authentication mechanism used to authenticate an individual or entity is responsibly managed and properly protected to prevent unintended use or compromise.
3) **Authentication Validation.** To confirm and validate the identity of an individual or entity upon presentment of the authentication mechanism to an Internet-based system.
4) **Application Security.** To ensure that an Internet-based application is properly insulated from direct access from the Internet, and that only individuals or entities whose identities have been positively validated are eligible to access the application.

All agency Internet applications residing on the state network that require authentication services must rely on Authentication Validation processes and Application Security services provided by Transact Washington or Fortress and the Washington State Digital Government framework or alternative processes and mechanisms which provide an equivalent level of confidence.

High levels of confidence are achieved by ensuring that stringent processes and controls are applied to all aspects of the authentication process. For example, this may require that an individual appear in person to confirm their identity before being issued an authentication mechanism. Trustworthy controls and technologies must be applied to protect the authentication mechanism and processes must be put in place to revoke or disable the authentication mechanism should it become compromised.

For applications with lesser risk or financial liability, owners may allow for the use of less rigorous authentication processes and controls.

Required Risk and Use Assessment Process
The Information Technology Security Policy requires agencies to identify applications that require the highest level of confidence of identity. This likely will necessitate that all parties interact through a common security architecture and authentication process.

Prior to choosing an identity confidence level, agencies must conduct and document an assessment of each of their Internet-based applications that addresses the issues identified below. (Suggested guidelines for conducting this risk assessment can be found in Section 6 of the Information Technology Security Guidelines.)

Step 1 – Documentation of Risk Issues
The agency risk assessment for Internet authentication must document the following:

- The potential impact of viewing data by unauthorized intruders
- The potential impact of unauthorized viewing of the data by otherwise legitimate users
- The potential impact of the use of the information assets for other than authorized purposes
- The potential impact of unauthorized deletion, modification, or disclosure of information
- The potential operational impact if the service becomes unavailable (denial of service attacks)

- The potential public confidence impact if the services or data provided by the system are compromised
- The importance of nonrepudiation (inability of a user to deny the initiation of a transaction) to the transactions supported by the system
- The impact of an intrusive registration and authentication process on the potential user base of the application
- The application impact on the potential user base due to one time and ongoing authentication costs

Step 2 – Assessment of User Base
Upon completion of the risk assessment of the Internet application, agencies must conduct an analysis of the application's potential user base. If some form of authentication is required, this assessment must address the potential for Internet-based users of the application to require access to current or future State of Washington Digital Government Applications.

If it is determined that the user base of the application would benefit from the convenience of single sign-on, regardless of the identity confidence requirements, the application must use the authentication processes and mechanisms supported by Transact Washington, or the agency must clearly document the operational and/or economic impacts which precluded the use of Transact Washington.

Agencies should consider the fact that Transact offers assurance level certificate-based authentication options. Agencies must choose the appropriate certificate assurance level for their application. Appropriate analysis of the potential future needs (i.e., higher assurance level certificates) of the user base should be considered in making this decision.

If users of an agency's proposed application have already applied for and received appropriate assurance level certificates for use with other State of Washington Digital Government applications accessed through Transact, agencies must accommodate these certificates if certificates meet the security requirements for the application.

Step 3 – Selection of Identity Confidence Level Processes and Mechanisms
After determining the risk associated with these issues, and identifying the user base of the application as unique, agencies must choose an authentication process and mechanism with attributes that provide the appropriate level of confidence for each Internet-related application. Internet applications that exist within the Washington State Digital

Government Framework (on the network backbone) must use the appropriate authentication processes and mechanism identified below.

- Transact/Certificate Policy/Shared Security Layer
- Fortress/Userid & Password/Shared Security Layer with appropriate agency processes for Identification & Authentication and Authentication Integrity

Agencies that use the Userid and Password services of Fortress must document how they address the Identification & Authentication and Authentication Integrity attributes below. Agencies may choose to use additional authentication mechanisms, such as SmartCards, beyond Fortress password protection. In such circumstances, agencies must document how these mechanisms will be integrated into the Washington State Digital Government framework.

If an agency chooses to use authentication processes and mechanisms to support its Internet application other than those supported by the Washington State Digital Government framework, it must document the following attributes of these alternative processes and mechanisms based on their cumulative ability to provide a level of confidence of identity commensurate with the application's associated level of risk:

1. Identification and Authentication

- User authentication mechanism request procedures
- User initial identification process
- User agreement format and content
- Authentication mechanism issuance procedures
- Authentication mechanism acceptance procedures

2. Authentication Integrity

- Authentication mechanism revocation procedures
- Authentication mechanism suspension procedures
- Authentication mechanism renewal procedures
- Authentication mechanism protection procedures (including specific vulnerabilities of the chosen mechanism)
- Obligations and liabilities

3. Authentication Validation

- Authentication mechanism validation processes

- System configuration

4. Application Security

- Network configuration
- Firewall configuration
- Intrusion detection procedures
- Audit procedures

F. IT Security Training

Agencies shall document the aims, training activities, schedule, and administrator for agency IT security training. The agency security program shall address regularly occurring training activities. Suggested guidelines for implementing security training processes, procedures, and practices can be found in Section 7 of the Information Technology Security Guidelines.

G. IT Security Program Maintenance

1. Agencies must have a plan to maintain their IT security program. This plan will require that agencies review, evaluate, and update its IT security policies, standards, and guidelines annually or more frequently whenever its business, computer, or telecommunications environments undergo change. Such change may include modifications to:
   - Physical facilities
   - Computer hardware/software
   - Telecommunications hardware/software
   - Telecommunications networks
   - Application systems
   - Internet-based information systems
   - Impacts related to organizational or budget changes

2. Pursuant to RCW 43.105.017(3), agency heads are responsible for the oversight of their respective agency's IT security and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be included in the agency IT portfolio and submitted to the Board. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval. The head of each agency must provide annual certification to the ISB by August 31 of each year that an IT Security Program has been developed, implemented and tested.

3. Agencies will assign responsibility for maintaining their security program. In addition, agencies will:

a. Document the procedure used for making changes to security processes, procedures, and practices

b. Provide procedures for distributing initial and updated IT security policies, standards, and guidelines

c. Agencies will have an audit performed once every three years for compliance with IT Security Policy and Standards. This audit must be performed by parties independent of the agency's IT organization. Each agency will be required to maintain documentation showing the results of its audit and plans for correcting material deficiencies that the audit identifies.

II. Standards for WWW and Web Browser/Web Server Configuration and Use

The Internet enables a number of services including e-mail, file transfer, login from remote systems, interactive conferences, news groups, and the World Wide Web.

This section describes the security standards for using the Internet and running state web-enabled applications over the Internet.

A. Internet Use and Connectivity

The agency's security program must address how the agency or employees within the shared network shall not establish permanent or sustained Internet connections via an ISP from a networked station that bypasses the DIS firewall. Such a connection provides an unmonitored backdoor from the Internet to the Washington State shared network that can lead to unintended security risks.

B. Minimum Web Client Security Standards

1. Web browsers provide a user interface to navigate through the Internet by interpreting, formatting, and presenting the documents to users. Browsers, e-mail clients, and other desktop tools may also introduce vulnerabilities to an agency. The following sections provide standards for the use of browsers.

2. Agencies must have a documented plan for the use and infrastructure associated with the use of web browsers and e-mail clients which adheres to the following:

   a. All software used to access the Internet must be approved by an authorized agency authority and must incorporate all provided security patches that are appropriate to the environment in which it is operating

   b. Only agency approved versions of browser software may be used or downloaded.

   c. All outbound browser traffic (beyond the agency intranet), will use appropriate technology to prevent disclosure of IP addresses

   d. If files are received from the Internet, ensure that files are checked for viruses by either:

1) Using anti-virus software on the workstation
2) Routing files to a repository server, checking for viruses, and forwarding the files to the appropriate workstation
3) Control of portable logic or interactive Internet technology (i.e., Java applets, ActiveX)

C. Web Server Security Standards

Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. There are many areas of Web servers to secure: the underlying operating system**,** the Web server software, server scripts, and other associated components. The agency's security program must address how the agency will ensure all agency Web servers adhere to the following standards for operation and maintenance:

Information placed on any Web site is subject to the same privacy restrictions when releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information. Agencies must conform to the ISB Public Records Privacy Protection Policy that implements Executive Order 00-03, Public Records Privacy Protections for its Web site information.

1. Users are forbidden to download, install or run Web server software without prior approval by an agency authorized system administrator.
2. Any remote control of Web servers (i.e., all administrator operations, including supervisor-level logon) shall be done from the console or properly secured sessions using high confidence level authentication.
3. Web server software and software of the underlying operating system shall employ all security patches and configuration options appropriate to the environment in which it is operating.
4. A public Web server should not serve as a repository for confidential data. A public Web server can act as a proxy for access to confidential data located on secure servers.

III. Standards for Digital Government (Internet) Application Submittal

A. General Requirements

This section describes the IT security related content that must be included in the submittals for Internet-based application design packets. The agency's DIS Senior Technology Management Consultant will use available internal and external resources to review design features relating to Internet security. The Consultant will provide developers pro-active access to the security infrastructure and provide development teams (particularly those agencies with no E-commerce security

personnel) with suggestions or advice on how to best utilize the security infrastructure. Both DIS and agencies will ensure that applications will run within the existing capabilities of the Washington State Digital Government framework.

Internet-based applications that are designed to provide anonymous access to public information (no specific application level security requirements) are not subject to this submittal requirement.

If a new application or data source is to be integrated into a previously submitted environment, no subsequent submittal is required.

B. Internet Application Design Packet Submittal Contents

The agency's security program must address how the agency will ensure all new Internet-based applications will be reviewed with the agency's DIS Senior Technology Management Consultant. In addition, the security program must address how submitted information will include, at a minimum, the following IT security related information:

- Application description - Provide a general description of the purpose of the application and the nature of the information involved
- Application services - Describe the nature of the services to be provided to the user of the application (static data, interactive queries, data entry, electronic payments)
- Authentication requirements (high, medium, low level of confidence) - Describe the level of confidence required for user authentication and provide a summary of the analysis completed to determine this level
- Certificate Authority integration (if required) - If the proposed authentication mechanism involves the use of digital certificates, describe any known application integration issues
- Application access control mechanisms - If the project involves providing access to an existing application, describe the nature of the application's access control mechanisms (user ID, password, etc.) If it is the intent of the agency to re-authenticate a user at the application level after they have been authenticated by a centralized mechanism and processes (such as Fortress), describe the justification for not accepting the initial authentication
- Encryption requirements - Describe any specific encryption requirements for data transmission and/or storage
- Proposed development tools - If known, describe the proposed development tools to be used in the creation or modification of the application for use via the Internet
- Proposed Web server platform - If known, provide information regarding the hardware, operating system, and services provided by the Web server platform

IV. Standards for Secure Management of Information

An Agency's risk assessment should identify which data is confidential and when that data needs to be encrypted (secured). The agency security program must include methodology to ensure that when data is designated as requiring encryption the following is met.

A. Secure File Transfer

Secure exchange of information from one application or user to another requires that:

1. All manipulations of data during the exchange are secure.
2. If intercepted during transmission, data cannot be understood.
3. The intended recipient is the only one who can understand the transmitted information.
4. Confirmation is received that the intended recipient received the data.
5. Confidential information subject to exposure must be encrypted.

It is assumed that the exchange of information occurs only between secure endpoints.

B. Secure Email

Secure delivery of a message from a sender to a receiver requires that:

1. E-mail, and any attachments, containing confidential information must be encrypted from the "sending device" to "receiving device".
2. Chain-of-custody to be preserved from "sending device" to "receiving device".
3. Ability to "unencrypt" sender's message through authorized process; sending organization must be able to un-encrypt" and retrieve originating version of sent message.
4. All manipulations of data during the transfer from sending device to receiving device are secure.

If intercepted between sending device and receiving device, data cannot be understood.

5. Only the selected receiver can view the data in its original, unencrypted state.
6. If technically feasible, confirmation is received that the intended receiver received the data.

The sending organization will determine what information requires the need for secure e-mail and the encrypted e-mail message is retrievable within a pre-defined archival period.

C. Secure Data Storage

Secure data storage is defined as the protection of data content and changes in data state from its original storage on electronic media by using encryption processes. Secure data storage requires that:

1. An organization has the ability to unencrypt stored data through an authorized process.
2. An organization has the ability to unencrypt stored data through a pre-defined recovery period identified by the organization.
3. An organization must protect the encryption and decryption method (key and algorithm).
4. If the data is accessed by unauthorized entity, it cannot be understood.
5. An organization has the ability to detect alteration of intended content.

V. Standards for Wireless LAN Access

The introduction of wireless as an alternative method to access an agency's LAN imposes new risks associated with unintended access and/or disclosure of data not only to an agency's network but also the risk of potential exposure to the entire State Government Network (SGN). The standards set forth in this section respond to the issues that must be addressed by agencies concerned with authenticating wireless users and providing these users with access rights to an agency's network. These standards must become an integral part of an agency's security program and the wireless tools and processes used should be appropriately documented.

Implementing wireless LAN access to state computing resources, requires agencies to:

1. Establish, document and communicate wireless access security practices within the agency.
2. Firewall all wireless access point connections from the agency network and the SGN.
3. Use industry standard authentication and encryption methods (See Section 5 b. Internet Access Security).
4. Agencies will perform a self-audit on a regular basis to locate any rogue wireless devices.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.